Privacy & Security Tiger Team
Draft Transcript
November 8, 2010

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director
Good morning, everybody, and welcome to the Privacy and Security Tiger Team call, which will run from 10:00 to noon. Just a reminder, please, workgroup members, to identify yourselves when speaking. There will be opportunity at the end of the call for the public to make comment. Let me do a quick roll call. Deven McGraw?

Deven McGraw – Center for Democracy & Technology – Director
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Paul Egerman?

Paul Egerman – Software Entrepreneur
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Latanya Sweeney? Gayle Harrell? Carol Diamond? Judy Faulkner? David McCallie?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Present.

Judy Sparrow – Office of the National Coordinator – Executive Director
Neil Calman? David Lansky? Dixie Baker?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Micky Tripathi? Rachel Block?

Rachel Block – New York eHealth Collaborative – Executive Director
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Alice Brown?

Alice Brown – National Partnership for Women & Families – Director HITP
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
John Houston?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Wes Rishel?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Leslie Francis?

Leslie Francis, NCVHS – Co-Chair
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Adam Greene?

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Lisa Teterough?

Lisa Teterough
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Did I leave anyone off?

Carl Dvorak – Epic Systems – EVP
This is Carl Dvorak. I'm here as well.

Judy Sparrow – Office of the National Coordinator – Executive Director
I'll turn it over to Deven and Paul Egerman.

Deven McGraw – Center for Democracy & Technology – Director
Thanks, everybody, for joining us today. We look forward to a robust couple of hours here. What we're going to focus on today is provider entity authentication. Our hope is to get through as many questions and try to reach consensus on some recommendations, as many of these as we can today. We did schedule another call this week because we otherwise would have had this call only between now and the next policy committee meeting.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Deven, it's Carol Diamond. I joined.

Deven McGraw – Center for Democracy & Technology – Director
We're going to try to be as efficient in having these discussions, but of course making sure that everyone has an opportunity to have their say. But again, our goal is we've got really only two meetings to get some recommendations in and down and consensus reached before the next policy.

With that in mind, I think we should just jump right in. Again, this is just making sure we understand the scope of our discussion, which is limited. That is to define policy recommendations to assure that authentication trust rules are in place for information exchange between provider entities or organizations. Then we have on our slide two reminders of some key definitions here: authentication being verifying that a now technically person or entity, but we're really talking about entities here, seeking access to electronic protected health information or PHI is the one claimed. Then, of course, level of assurance is a degree of confidence in the results of an authentication attempt.

We really need to focus on the directed exchange transactions that are in stage one of meaningful use, but we should consider other information exchange transactions in our deliberations. We assume that identifiable clinical information is going to be transmitted from one provider entity to another, particularly for treatment and care coordination purposes in stage one of meaningful use. Of course, some of this information that's being transmitted is going to be very sensitive to the individual. On these next two calls, we're evaluating these trust rules at the organization level, so the scope of this recommendation does not include authentication of individual users within these organizations or patients with respect to their ability to electronically access their information. It's not as though we don't think that these are important, but that's not the scope of this initial set of recommendations that we're trying to scope out here today. We assume that with respect to provider entities, they are going to need to have policies to identity proof and authenticate their individual users of their system. Certainly for more robust exchange, the policy of individual user authentication, we may need to do more on this issue as individual users, and we certainly already know that patient authentication and access to date is on a short-term list of issues that we need to take on in the future.

We wanted to make very clear that our discussions today are machine-to-machine authentication, EHR-to-EHR, and not down to the individual user level. We sent you this morning a very brief summary of some of the comments that we got on the federal advisory committee blog since the comment period was extended, and it really just closed on Friday. This was sort of the best that we could do to get you a sense of where the comments are quickly before this call, which you didn't get very much in advance of it, so thankfully you'll have more time to read it for the second call. The folks from MITRE who help us out are going to get us a more detailed summary. Of course, all of you can access those comments on the blog as well. We got a very interesting set of first round comments on the proposed questions that we sent out, but I will say, having looked through them, many people didn't understand that in fact we were focusing at the entity level and not down to the individual user, and so as a result, I think some of the comments that we got are probably, we're going to have to hold them in check for when we take up individual identity and authentication in subsequent meetings.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I assume, but I'd like to hear you confirm, and also we may articulate it that we are not assuming that there's one entry point to an organization, right?

Deven McGraw – Center for Democracy & Technology – Director
No, I don't think we're assuming that at all, but I think we are assuming a single system within an organization, so it might have multiple entry points, but still the same system. Paul, do you have—?

Paul Egerman – Software Entrepreneur
Actually, it doesn't even necessarily have to be a single system. It's probably a single system, but I don't think we have an assumption that there's one entry point and one system. It would certainly be easier, but I think there are a lot of environments where it's a little bit trickier if you look at something like an imaging center or maybe an imaging center is a good example where it might have multiple locations. Each location actually could have its own entry point, if I understand your terminology correctly, Dixie.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think, in most cases, an entry point—to authenticate an organization, let's say, what you're really going to authenticate is a gateway into the organization, like NHIN Connect … organizations that use NHIN Connect. But there are gateways into multiple organizations. I think that we should make it clear that a single organization could have multiple gateways. Let me ask you a specific one. If you have a Kaiser or Mayo where they have multiple sites, I'm assuming each site would have a different identity, but a single site could have multiple entry points into that site. Is that right?

Paul Egerman – Software Entrepreneur
That's right, although we have to be careful. We're getting perhaps a little bit too far into the details a little bit too soon.

Deven McGraw – Center for Democracy & Technology – Director
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's reality though.

Paul Egerman – Software Entrepreneur
It's reality, but there's nothing that we're saying that prohibits that. One of the confusions is we are sort of very loosely defining entity and organization.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I think that there is going to be a certain amount of detail that unfortunately we're going to have to get into, even in this type of a discussion because there are so many permutations of organizations out there. I know that from my personal experience, we deal with often where we have a joint venture with another hospital where we have a common location. I understand … detail, but boy I'll tell you. That's the type of stuff people are going to start asking questions about real quick.

Deven McGraw – Center for Democracy & Technology – Director
Yes, undoubtedly, but I think we should think, as we always do, about how to set organizational authentication policy that would ideally be flexible enough to accommodate different arrangements.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
What I hear is that we are not making an assumption that there is a single system that controls all passage of information into and out of an organization, right?

Paul Egerman – Software Entrepreneur
That's correct. That's not necessarily an assumption.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I'm saying is this specifically what you might call a non-assumption? That is, we're assuming the contrary is possible.

Paul Egerman – Software Entrepreneur
That's correct.

Deven McGraw – Center for Democracy & Technology – Director
Anything else before we start to dive into this discussion that we seem to already actually be diving into?

Gayle Harrell – Florida – Former State Legislator
If we are not assuming that there's one entry point into an organization, then are we going to have to say you have to authenticate each entry point? Where does that lead us?

Paul Egerman – Software Entrepreneur
The answer probably is yes, you have to authenticate each entry point.

Deven McGraw – Center for Democracy & Technology – Director
I think that's right. Why don't we? My suggestion is that we think about the range of those possibilities when we sort of get to the question of organizational authentication and an acknowledgement that there could be more than one system and more than one entry point, and how would we approach that from a policy standpoint? Welcome, Gayle, and congratulations.

Paul Egerman – Software Entrepreneur
Yes, congratulations, Gayle.

Gayle Harrell – Florida – Former State Legislator
Glad to be representative again.

Deven McGraw – Center for Democracy & Technology – Director

This slide is just a review of the set of questions that we have put forth in previous phone calls and that they were also the questions that were on the FACA blog, and it's these questions that we're going to try to power through as much as we can today and pick up where we left off in our subsequent meeting on Friday, and they deal with strength of authentication, which provider entities can receive digital credentials, and what requirements should they have to meet. What is the process for issuing these credentials, including evaluating initial conditions, as well as reevaluation? Who has digital credential authority, authority to issue them? Should the Office of the National Coordinator select and establish technical standards? Should that standard or set of standards be required as part of EHR certification? What types of transactions need to be authenticated? Is it expected that all transactions would have a common level of assurance?

With that, setting some, what we think are, assumptions for this conversation, that because we're talking about organizational level authentication, what we're looking to validate is that the computer is linked to the right organization. The organization is who it says it is. Do they really exist, so that we can insure there isn't any spoofing or assumed identities for malicious intent? Even where the relationship is reliable, we need to be mindful of the consequences of getting this wrong of an authentication error.

Again, for stage one of meaningful use where the exchange requirements are not quite as robust, although I think we all expect that they will become more robust in stages two and three. It is likely that the exchange is going to involve the sender and the recipient having some sort of relationship. So the entities maybe are more likely to be known to one another. Now you folks can push back on that assumption, but again, for the lightweight set of transactions that we're talking about for stage one, we are at least in our discussions that Paul and I have had, we think that there's an assumption that the entities are more like to know one another, even if their computer systems don't necessarily know one another. But that could be likely to change in stages two and three.

Then with those assumptions and the discussion that we've already had about an assumption that we didn't put on the slide, but the likelihood that organizations could have, that there could be more than one system and more than one entry point, we can move into the first question, which is about level of assurance. I'm turning it over to Paul for this one.

Paul Egerman – Software Entrepreneur
Yes. Thanks a lot, Deven.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I have another question, Paul.

Paul Egerman – Software Entrepreneur
Before we do that, on the previous slide where we had assumptions, we should add the comments that were made that the assumption is not necessarily the case that each organization has only one gateway.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Paul Egerman – Software Entrepreneur
There may be multiple gateways, so we'll add that to the list of assumptions. I'm sorry. Go ahead, Dixie.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I was just wondering. It doesn't say, but are we still talking about directed exchanges, or are we talking about the full scope of exchanges for state one?

Paul Egerman – Software Entrepreneur
I think we're still talking about directed exchanges.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think we should say that somewhere as well.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Can I ask a quick question as well?

Paul Egerman – Software Entrepreneur
Sure.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I know this may be putting the cart before the horse a little, but is there an assumption that an entity that we would be authenticating would also be going through a process of assigning a DURSA, or is that maybe a recommendation we would make as part of the process?

Paul Egerman – Software Entrepreneur
It's a great question, but that's one of the questions that we will be answering today, and in the next meeting. We have these six questions that Deven just went through, and one of the questions is which organizations, or Wes had a better way of phrasing it, what are the characteristics of an organization that will receive some digital credential? So that that could be one possible answer is what you just suggested, John. That's a great question. I think that's question number four. We will get to that question.

What we're trying to do today is to start to answer these questions and come up with responses to the questions. That's our agenda for today. We have these six questions. Now Deven made reference to the public comments on the blog, on the FACA blog, and there are 58 comments. What I would encourage all the tiger team members to do is to do the same thing that I did, which is just to sign on and read every one of them.

We did do our best. The good people at MITRE put together a short summary to help you where we tried to organize all the responses by question number, but that's a very short summary. When you read the actual comments that are coming in, there are 58. It's very interesting. First of all, it sort of reminds, at least it reminded me of the importance of the work that we're doing. The fact that 58 people took the time to write thoughtful comments, there are a lot of people who are very, very interested in this work and have very strong opinions on it.

But that's also very important, but there were some great comments that were made, and just to reference a few of them, and also it's very important what Deven said. There was clearly some confusion about individuals versus organizations. One area that came up in the AHA comment, Laurence Hughes wanted us to be clear that we're talking not about information exchange within an organization, but rather between organizations. So this is not within organizations, but even within multiple sites of an organization. This is from one organizational entity to another. Now, of course, in healthcare, it's hard to know what an organizational entity is, but that's what we're talking about, so that was very helpful that the AHA pointed out that issue.

Again, as you read through it, this issue about provider entity organizations versus individuals is sort of like a recurrent theme, and there's a lot of confusion, although there were some people who clearly understood what we were talking about. Shirley Neil, I guess, from Allscripts put in a couple comments that were very helpful in terms of clearly delineating that issue. One of the comments actually also that I liked a lot came from a person named Jeff Maynard who wrote there is no perfect authentication scheme. I read that, and I said that's something we also need to remind ourselves of, as we go through this whole process. We're trying to come up with an authentication scheme, but this is not perfect, and it's not the sole security measure. There are lots of other things that will be going on, so we need to keep those concepts in mind.

Having said all that, we looked at this issue of question number one, which was sort of like what is the level of assurance … authentication? I read through the blog entries, as they were coming in, and then we actually had a number of conversations with people at ONC, Deborah Lasky, and people at MITRE on this issue. We sort of came to the realization that we're sort of like asked the right question, but it's like in the wrong place. The level of assurance question is really a question that belongs when you're authenticating individuals or individual users that when you're talking about digital credentials for a computer or a machine or what Dixie called a gateway is really not so much an issue of level of assurance. In fact, there's really only like two or three existing standards that one could choose from, and that this is not really the right question to be asking at this point, although we will return to this question when we get to patient access and when we get to issues of user access.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I don't agree with that. I think we still, it's not addressed in the same way, but we still have to address assurance because you can't have me calling up and asking for digital certificate and claiming that I'm Mayo Clinic.

Paul Egerman – Software Entrepreneur
That's right, but that's the process of obtaining the certificate. We're going to address the issue that you just described in a minute. I'm sorry. Wes, were you trying to say something?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I think we're having considerable confusion between the act of authenticating that occurs just immediately prior to communication and the act of issuing credentials.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I agree. I think so too.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
There's certainly no reason why we can't be talking about the level of assurance for the act of credentialing.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Paul Egerman – Software Entrepreneur
That's correct. In other words, that's an excellent comment, Wes, because when we originally drafted this question, we were thinking of level of assurance like the four levels of e-authentication. But when we read though all the detail on that, it was like it wasn't appropriate because it was talking about things like biometrics. That's not what belongs here, but what we do need to do is exactly, I think, what you just said, Wes, is what is the … issuing the credentials.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's exactly what I just said as well.

Paul Egerman – Software Entrepreneur
Okay. I agree with that, and so those are the key issues is so like who is going to get these credentials, and how are we going to decide, as you suggested, Dixie, that it's not you or me calling up and claiming to be Kaiser and getting one. How do we do this correctly? Are there other comments on this issue?

Deven McGraw – Center for Democracy & Technology – Director
Is it safe to say that what we seek is actually a high level of assurance that the organization is who is claims to be?

Paul Egerman – Software Entrepreneur
Yes. You need a high level of assurance on the identity of the organization before the credentials are issued.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

I think the question is not do we want high, but how high. It's easy to imagine approaching perfection in this by sending an inspector out to deal with every single admission, and I think it's an open question whether we want to do that or not.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Deven McGraw – Center for Democracy & Technology – Director
But doesn't that get to— It's almost as though answering some of the subsequent questions on the list like who is eligible to get a credential, and what do they have to prove, and who do they have to show it to is all sort of wrapped up in this question of how high, right?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's right.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes. Like all of these, there's a certain amount of iteration that goes on, but I think the sequence is right. We should go in this sequence, recognizing they have to iterate a little bit.

Paul Egerman – Software Entrepreneur
Yes. The first part of that sequence I'm hearing is we don't know what the definition of high is, but we want to have a high level of confidence in the identity of the organization before the credentials are issued.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I would say like everything in security, we want to have a balance between the level of assurance and the cost that is an acceptable tradeoff. When I said the sequence was right, I was thinking of the three questions about the credentialing process, which entities get credentialed, what's the process, and who can be an issuer.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
From the discussions on this topic that occurred on and off the last few months with the NHIN Direct or Direct Connect project, which I'm just raising as an example, not that we're necessarily solving that specific question, but one of the things that kept tripping us up was the distinction of assurance of the identity of the other person versus do you actually want to communicate with that other person? Who should get a credential is a very different question than how do you make sure that the person who got the credential is who they say they are? Does that make sense? Just keep those straight.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Just replace entity with person here in that, right?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. No, when I say who, I mean entity. In other words, the technical assurance that you are in fact talking to the person, to the entity that you think you're talking to is one question. Who should you be allowed to connect to is a completely different question. E

Paul Egerman – Software Entrepreneur
I agree.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
They get blurred sometimes.

Paul Egerman – Software Entrepreneur

I agree, but we're only talking about the first one.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. I agree.

Paul Egerman – Software Entrepreneur
… make sure that ….

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, how do we …?

Paul Egerman – Software Entrepreneur
… picking up on Dixie's expression of the gateway. We're just trying to make sure that you're ringing the correct doorbell in terms of who you intend to talk to, but you're not necessarily knowing who is going to answer the door and whether or not you're going to get the person you want to answer the door.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, I'm talking about the doorbell. Yes, I agree.

Paul Egerman – Software Entrepreneur
Any other comments about this first question before we dive go through on a layered basis, to pick up Wes' comment? Not hearing that, we'll start into the next question, which we divided in half. Am I doing this one, Deven, or are you doing this one?

Deven McGraw – Center for Democracy & Technology – Director
You can keep going, Paul.

Paul Egerman – Software Entrepreneur
Okay. Which says, which provider entity should receive, and then it says, or be issued digital credentials? The reason why it says that in parentheses is it was rightly pointed out that when we wrote the questions, you don't really receive the digital credentials. They're really issued to you. We phrased it badly, but we did not want to change it in our call because we'd already put it on the public blog. So what we did was we sort of corrected it in parentheses, and you'll see that a little bit.

What you see, it says which ones. We didn't quite pick up—we should have—the terminology suggested by Wes at the last meeting, but we're really talking about what are the characteristics of those. What we have listed here is like a straw man answer. These are just some things that were just thrown out as ideas about who might get these. So it's not intended to be all inclusive list. There might be overlap in the list. It's just a number of comments. It's put here to generate discussion, so what do people think?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I noticed that on the public blog, somebody just said whoever is a covered entity under HIPAA. I think that is who we're talking about.

Paul Egerman – Software Entrepreneur
It could be broader than that. I think it's the business associates of those covered entities as well.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, right. Yes, but I don't think we need to create our own definition. We should base it on who can really exchange clinical information, and they all would be covered entities or business associates.

Paul Egerman – Software Entrepreneur
Let me ask a question about that. Is it all business associates?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
If they're exchanging PHII.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
And they don't have to be business associates if they're not.

Deven McGraw – Center for Democracy & Technology – Director
It seems to me, if we're going to set up some criteria that we think applies to the authentication of entities exchanging information in this space, wouldn't we want to frame it as, if you're going to exchange electronic protected health information, you should be required … digital credential according to these processes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
We're only talking about the exchange of information for treatment right now, right?

Paul Egerman – Software Entrepreneur
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
… going to be covered entities ….

Deven McGraw – Center for Democracy & Technology – Director
That's stage one, so if you thought about setting rules for meaningful users, then you would know that the universe would be relatively confined to that space, although certainly there will be lots of meaningful users with a much higher degree of sophistication in terms of their exchange practice.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
For stage one, it would also include PHRs for stage one because that's stage one as well, right?

Deven McGraw – Center for Democracy & Technology – Director
Right, but we deliberately said that we would do patient identification separately.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No, I'm not talking about the patient. I'm talking about PHR provider.

Deven McGraw – Center for Democracy & Technology – Director
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That ought to require a covered entity to be able to send clinical information to a PHR provider entity.

Paul Egerman – Software Entrepreneur
Let's back up a minute. We talked about covered entities and business associates. Then Dixie said PHR provider. A PHR provider is neither a covered entity nor a business associate. Is that correct?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right.

Paul Egerman – Software Entrepreneur
We now have three groups: covered entities, business associates, PHR providers.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Then stage one also includes immunization registries, at least to the level of test transactions. I think we would argue that there's a set of entities around public health.

Paul Egerman – Software Entrepreneur
Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
That unless they happen to be treatment providers or payers, aren't necessarily covered entities.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Paul Egerman – Software Entrepreneur
Public health agencies or entities?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I prefer to say entities at this point.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Paul Egerman – Software Entrepreneur
Okay.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
We might have to decide what an agency is.

Paul Egerman – Software Entrepreneur
Then what about what's written here? It says non-providers, payers, claims clearinghouses, HIOs.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Covered entities.

Paul Egerman – Software Entrepreneur
Those are all covered entities?

Deven McGraw – Center for Democracy & Technology – Director
Yes, well ….

Paul Egerman – Software Entrepreneur
HIOs are not.

Deven McGraw – Center for Democracy & Technology – Director
That's a business associate.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Business associate if they have clinical information.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO
How are HIOs different than the second bullet? I'm not sure I understand health data exchanges.

Paul Egerman – Software Entrepreneur
That was just thrown out as the straw man. What the group seems to be saying is they're given a shorter list and a different list. They're saying covered entity, business associate, PHR provider, and public health entities is what they're saying. Now I'm trying to say, are we leaving anything out? What about CME?

Deven McGraw – Center for Democracy & Technology – Director

I have a suggestion. Rather than try to look to the entire universe of possible exchangers for this recommendation, what I suggest is, especially given that the recommendation is going to be the Office of the National Coordinator, that we say something about any participant, anyone who is going to be part of a data exchange, whether on the sending or the recipient side, under the meaningful use program, should be required to have a digital credential. Ideally, even outside of the meaningful use program, this ought to be a sort of exchange requirement for any player in the healthcare system who is going to be exchanging EPHI.

Paul Egerman – Software Entrepreneur
Right, although that gets us a little ahead of the questions, Deven. We have a question about developing standards and ….

Deven McGraw – Center for Democracy & Technology – Director
No, I get it, but in terms of which ….

Paul Egerman – Software Entrepreneur
… certification.

Deven McGraw – Center for Democracy & Technology – Director
I understand that, but I sort of am, I guess I'm pushing back on trying to create some sort of exhaustive list here, and instead shooting at a policy recommendation that says really anybody exchanging EPHI ought to have a digital credential.

Paul Egerman – Software Entrepreneur
Yes, but let me ask a question, which is, do we want to narrow it? Do we want to say that if you're what I would call a treatment provider, you have to have a certified EHR system in order to receive one of these digital credentials? In other words, if you're a hospital or group practice, and you have a system, but it's not certified, you can't get one.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I don't think that's reasonable. I know we're trying to focus on meaningful use, but even entities without an EHR have to report public health. But are we not considering …?

Paul Egerman – Software Entrepreneur
They might have a different credential than the one that we're issuing.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Can I suggest that I think it's of value to list out all the different types of entities like we're discussing, because if we don't, I fear people looking at this may start to ask questions about what is the scope? So I think it helps to inform people as to really where our head is and what the scope of this is.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But do we want to include law enforcement?

Paul Egerman – Software Entrepreneur
I don't think ….

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
No.

Paul Egerman – Software Entrepreneur
No.

Leslie Francis, NCVHS – Co-Chair
No.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's just a different category entirely.

Leslie Francis, NCVHS – Co-Chair
It's a different barrel of fish.

Paul Egerman – Software Entrepreneur
It is a totally different situation, but I think most law enforcement is not doing electronic exchange with HL-7 right now. Maybe they are.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
From their cruisers.

Paul Egerman – Software Entrepreneur
Yes, right. I'm sure one can make a number of comments about that, but the question that I had asked was, and maybe this is a question that can deal with when we get to some of the later questions, is to also realize that there might be an issue of enforcement with the issuance of these credentials. In other words, if you say you have to have a certified EHR system, well, that's a way to give a level of maybe enforcement or level of assurance that whoever you're sending and receiving information with does have certain internal security measures or does have a certain amount of consistency with how the transactions are going to be formatted.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But you can't tell someone with an EHR that they can't send health information to somebody that doesn't have a certified EHR. I think that would go against what we're trying to achieve.

Paul Egerman – Software Entrepreneur
Maybe you can't send it through the NHIN. You have to send it some other way.

Deven McGraw – Center for Democracy & Technology – Director
Yes, but even within stage one of meaningful use, there are a class of entities that are going to be involved in exchange transactions, like the immunization registries, like state public health entities, like laboratories that are not going to have certified EHRs.

Paul Egerman – Software Entrepreneur
I agree, but I'm just saying for the ones that should. Were you trying to say something, Gayle?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
No, this is Carol. I was just going to say, we have to assume a level of asymmetry that there might not be an EHR at all.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, exactly right.

Deven McGraw – Center for Democracy & Technology – Director
Right.

Paul Egerman – Software Entrepreneur
Well, I don't agree with that, Carol.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
The whole point of NHIN Direct ….

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
At the receiver end.

Paul Egerman – Software Entrepreneur
How is it going to read an HL-7 transaction without an EHR system?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It may not be an HL-7 transaction.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, it could just be text about the patient or consult.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, it could be e-mail.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
We can't prevent the information from flowing just because a provider doesn't have an EHR. We have to assume that there's an asymmetry of applications, and none of this can hinge on whether or not someone is using a particular application. It should hinge on whether or not they're capable of receiving the information securely.

Paul Egerman – Software Entrepreneur
Right, but we're talking about, for example, stage one of meaningful use. If you want to send a CCD or a CCR, you've got to have some computer system on the other side to receive it. It's not readable.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
But it could be a HISP, for example.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
You could argue that, I think, that a very strict interpretation of stage one meaningful use would rule out non-EHR, but I hope we can come to a solution that's not— One of the whole things we've been working on is separating these layers, not tying the standard for formatting data to the way we send it around. I sure hope we can avoid creating a dependency here.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I agree.

Deven McGraw – Center for Democracy & Technology – Director
Yes. I think that makes sense. We certainly have a lever in certification to make sure that the systems that we're spending federal dollars on have the capability to be appropriately authenticated and digitally credentialed. Having said that, if we just focus our policy on certified EHRs, I think we'll miss a broader universe of what we hope will be exchangers of PHI for treatment purposes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Right. I think all these entities on here should fall under this recommendation, and many of them aren't EMRs.

Paul Egerman – Software Entrepreneur
Okay.

Deven McGraw – Center for Democracy & Technology – Director
Right, so if we started with a global recommendation that any entity that is involved in the exchange of patient identifiable data ought to be digitally credentialed, and this is sort of a universe of entities that we would include in that list. It's not necessarily mutually exclusive. Certainly it ought to be the case for providers using certified EHRs. That's a potential policy lever for making sure that the systems are able to be credentialed.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Deven, I like that formulation, but can I ask a technical question just to get a sense of where you're going?

Deven McGraw – Center for Democracy & Technology – Director
You can ask one. I'm not sure I'll be able to answer it.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I apologize again for getting concrete, but I just want to test. When you say digitally credentialed, would you consider two entities that had established a virtual, a VPN, to qualify at digitally credentialed? Of course, that's the common way these things are done today.

Deven McGraw – Center for Democracy & Technology – Director
Right.

Paul Egerman – Software Entrepreneur
I think the answer to that, David, is going to come when we talk about who issues the credentials.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Arguably, if there's a private link between two entities, they've decided that there's a trust relationship that's been established.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Paul Egerman – Software Entrepreneur
Yes, so they have a different kind of credential than what we're talking about here.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Exactly.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
But would we be saying that they need to go get a different kind of credential that they couldn't just establish a VPN using, I'll call it, traditional approaches, which are obviously quite secure?

Paul Egerman – Software Entrepreneur
What we might be saying is that in addition to that, they also have to have one of these.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think that's a big impact.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I think it's only at the point where there's a decision to participate in a public exchange. I'd hate to say it that way, but some type of exchanges where you have to get the credential. If parties decide to privately exchange data, I don't think that we should be advocating that they have to be credentialed.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
It seems to me, that's a pretty big assumption to tease out. I'm not saying I disagree with it, but I just think that the vast majority of the PHI exchanges today are privately established using either SSL or VPN or both.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

When I talk about private, I'm talking about private parties. Two organizations have chosen to exchange data ….

David McCallie – Cerner Corporation – Vice President of Medical Informatics
But that is the essence of directed exchange.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO
I don't see how you can carve those out from the way we've defined all of this up until now.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I don't think you can either. In fact, to Carol's comment, then you'd have to tease out the asynchronous exchanges. I think we should just address it as health exchanges for treatment purposes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Then maybe when we enumerate the ways in which one can establish a secure credential channel that we might include VPNs established privately or something like that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Even with a VPN, you need to credential at each end.

Paul Egerman – Software Entrepreneur
That's right, but I don't understand your concern, David. Your concern is?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Well, Deven's language of issuing or being digitally credentialed, I guess I'm asking what the scope of digitally credentialed is in terms of the way people do things today. Most people are not using SAML today, but one could interpret digitally credentialed to say that's the way you want to do it.

Paul Egerman – Software Entrepreneur
Let me suggest, we're going to get to that issue because, again, the question that we're asking, let's just stay focused on the question, is which provider entities should receive or be issued digital credentials? Let's put aside for a moment what's going to happen with the certified EHR systems because I think we have an agreement on the answer to that question, which is, we said it's people are involved in health data exchanges. We talked about covered entities, business associates, PHR providers, public health entities, and then John Houston's suggestion was also to list out these as examples so that people know what we're talking about too, can see the scope of what it all means, and I think that's a good answer to this question.

Deven McGraw – Center for Democracy & Technology – Director
Yes. Let's hold the VPN question in our hip pocket.

Paul Egerman – Software Entrepreneur
Well, the certification. It's really a question about requirements and certification is where we're tripping up right now.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
We're really addressing how you get the credential, and we're not addressing at all right now the transport between it, whether ….

Paul Egerman – Software Entrepreneur
Yes, that's correct. But this question, 2A, is simply which entities should be issued the credential?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I totally agree with the list you just read off, Paul.

Paul Egerman – Software Entrepreneur

Okay. So my question is, are we comfortable with that as an answer for question 2A and ready to move on to the next question?

Deven McGraw – Center for Democracy & Technology – Director
Yes, and we'll formulate it for our next meeting so people can see the language.

Paul Egerman – Software Entrepreneur
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, I'm comfortable.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Paul Egerman – Software Entrepreneur
Everybody okay? Then let's move on to the next one, 2B. I'm still confused. Are you doing this one, Deven, or am I doing this one?

Deven McGraw – Center for Democracy & Technology – Director
You can keep going, Paul. You're doing well.

Paul Egerman – Software Entrepreneur
Now we get into some of these interesting issues that we talked about before, which is, what are the requirements to be issued these credentials? In other words, what has to be true of the organization to be issued a credential? Now you see this issue. These are like straw men. These are suggestions. Valid licensure, I assume that would mean like the state license healthcare organizations. Business validity, this is the issue we talked about question one, proof of address, existence. Financial account, I don't know what that's there for. Demonstration of certain security criteria, here again having this EHR, if applicable. There might be other requirements. So what do we think about this?

Deven McGraw – Center for Democracy & Technology – Director
Thinking. There are sort of a lot of elements suggested on this list here, but I wonder if one of sort of overarching, one common thread here is really, at a top level, proof that there's actually an entity that exists, so whether it's a proof of corporate existence or the existence of a financial business account, corporate or personal tax returns in the case of partnerships. Then when you talk about licensure, that's probably only relevant with respect to entities that are required to be licensed in order to operate.

Paul Egerman – Software Entrepreneur
That's right. Licensure is a good requirement to the extent it's required. Looking at like perhaps a laboratory or something that's licensed, then it's a good requirement. But I think, in many states, group practices don't have to be licensed.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. I would say licensure is not on this list.

Paul Egerman – Software Entrepreneur
I'm sorry. You say it would not be on the list?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Right, I mean, I think that's an independent question. When you establish the trusted relationship with the other entity, they either do or don't have to be licensed, but it doesn't have anything to do with establishing the trusted relationship.

Paul Egerman – Software Entrepreneur

The issue though is can anybody get one of these digital credentials? Can I say I'm Dr. Smith and Jones and get a credential? Can I?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think that that's a function of what kind of interchange needs to happen.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
If the party is appropriate for this kind of interchange then yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'd like to address ….

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I think we're really at the fundamental question here, which is, how much are we expecting to rely on this process to assure that the decision point I make as a provider, for example, in establishing a trusted relationship, to be sure I'm relieved of due diligence. I think it's a question that has a lot of cost implications. I would argue that in terms of establishing the existence of the business or the person in case that the entity was a person. I don't mean a person within an entity. I mean an entity that equals a person. Banks have a set of procedures and standards that are sort of a floor for what she would be considering if she couldn't get a bank account as this business based on the rather modest requirements you have to do to get a bank account, you shouldn't be able to get one of these certificates. I don't know that that's sufficient, but it's certainly a start.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Why can't we just use the national provider identifier?

Paul Egerman – Software Entrepreneur
Wait. That's for individuals. We're talking here about organizations.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I thought that's for organizations as well.

Deven McGraw – Center for Democracy & Technology – Director
It is.

Paul Egerman – Software Entrepreneur
There are many legitimate healthcare concerns that don't have a national provider identifier issued to them.

Judy Faulkner – Epic Systems – Founder
I joined a little late, but I have kind of an overarching question that you can slap me down for if you think, which is, isn't there a huge difference between sending the entire medical record to another place that the patient shows up versus sending information about the lab test to the lab and getting the results back? Aren't there really two levels that we need to consider?

The second, the organizations have been doing well by themselves for years. They send it to the lab. They get the lab test results back. But when I hear people talk about interoperability in general, mostly they're talking about, if I go somewhere else, I want my medical record there. Should we separate the two?

Deven McGraw – Center for Democracy & Technology – Director
Judy, we do have a question in the stack towards the end about whether there ought to be different levels of assurance, I think is the specific question. Different type of information, and you could sort of expand

that out to different processes in place. I don't know the answer to that question, but we do have a space to talk about whether we're talking about sort of one set of criteria across the board or whether we would create different criteria based on the type of exchange, whether it's whole record versus test results.

Judy Faulkner – Epic Systems – Founder
Sure. I'm worried that we're going to get bogged down … already works well. I send data to billing. I send information to lab. I send it to radiology. I get it back from all of them. It works well.

Deven McGraw – Center for Democracy & Technology – Director
Yes, I think it works in some context, but not in all. If we had the exchange thing licked, we wouldn't be having these conversations. But I think it's a good point to raise that we're not writing on a blank slate.

Judy Faulkner – Epic Systems – Founder
We're not writing on a blank slate, and I'm not aware, and you can correct me, but I'm not aware of the billions of stuff that goes on probably daily that I've seen newspaper articles saying they didn't send it to a lab, but was really some other place that got this data and ran off with it. I think the challenge is sending data from one organization that has most of the record to another, even if it's a private physician. I think the more the provider-to-provider thing, and if we concentrate on that and can do the other later. But the big one, I think, is the provider-to-provider.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think, Judy, that you've moved downstream and you're into the authentication piece. We're still back on how they get. You may know that that's the lab you use all the time, so that's authentication. But we're talking about how that lab gets the credential to begin with.

Judy Faulkner – Epic Systems – Founder
But then let me ask you a question, which is, is there a problem?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Deven McGraw – Center for Democracy & Technology – Director
Only in the sense that we do have entities today that don't have these credentials that have never really digitally exchanged. We have a lot of them.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Deven McGraw – Center for Democracy & Technology – Director
It may not be a hard problem to solve, but I think it's one that we need to make sure there's a process in place in order to make sure this happens.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think PHI is PHI. It's going to be hard to tease out based on the complexity of the message whether it should or shouldn't qualify.

Deven McGraw – Center for Democracy & Technology – Director
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Even though not every organization has an NPI, could we use the same criteria that they use to issue organizational NPIs?

Paul Egerman – Software Entrepreneur
Let's look at Judy's question about exchanging and looking at it in the context of stage one, exchanging a patient summary. Suppose we're at a group practice, and we get a message somehow that a hospital in

another state, a hospital we've never heard of before, wants a patient's summary, a CCD or a CCR on a patient. How do we know that that hospital really even exists that's not being …?

Judy Faulkner – Epic Systems – Founder
Yes, I think that's the bigger question.

Paul Egerman – Software Entrepreneur
Isn't that the question we're trying to answer? How do we know that's really Hospital ABC in some state we've never heard of?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I think this is what David was warning us about a little bit at the start of the call. The way we know now is our records room accepts a phone call. They sound like they know what they're talking about. They take a fax number. They maybe get a fax form in that claims to be the patient's signature on it, and they send it off, right?

Paul Egerman – Software Entrepreneur
Yes. That's terrible security, but that's how it works.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Right. We have the question, does having a digital mechanism for transmission that still involves people in the loop make it any worse or not? Normally we think that digital exchange amplifies the security threat. It's not clear to me that it does in this case, in the particular use case you describe there. It would, I think, it would never be presumptive. I don't know that you'd say— You could say presumptive. It would be presumptively true that you can send this data to the hospital just because they have a certificate, but it would certainly narrow down the range of the number of vulnerabilities you have to false claims if they have.

Paul Egerman – Software Entrepreneur
But think about it in the context of what John Houston said. He mentioned the DURSA, talk about NHIN Exchange. My understanding the way NHIN Exchange works, you sort of have a sense of confidence. You know who are all the participants.

Deven McGraw – Center for Democracy & Technology – Director
Right.

Paul Egerman – Software Entrepreneur
The question is, is this certificate working the same way? You somehow have a certificate. You have a set of confidence that there's some set of minimum criteria that is known about them.

Judy Faulkner – Epic Systems – Founder
The reason it works okay for things like billing and lab and stuff like that is because I end up as the healthcare organization having to pay them, and I know who I'm sending it to because I've got, in most cases, a known entity because they have to work for me. Whereas, when the patient goes to another healthcare provider, or says he or she does, that's the one I don't know.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
But I think if we allow for a variety of ways to achieve a credentialed conversation, which could include the simple VPNs that are in such common use today, then we're covered, as long as we include it in our list of accessible approaches. What you can't do is to get into the mixing of professional competence with possession of a credential.

Paul Egerman – Software Entrepreneur
No, we're not trying to mix professional competence. I'm just asking the question, can you assume there's some certain level of checking that occurs that the hospital really exists, or that's what this question is all about. Is there some minimum requirement to get one of these credentials?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
You asked the question that is the DURSA the model for this, and I feel compelled to answer that question. The DURSA, last I heard, is a legal agreement signed by all parties in a consistent form with a specific approach to modifying the agreement associated with governance. That approach says we're fine for a dozen entities. It's contemplated to work for a few hundred entities, but there's no possibility that it's going to work for hundred thousand entities.

Paul Egerman – Software Entrepreneur
I agree with what you just said, Wes. I use the DURSA as an example. I didn't mean to suggest that that was the solution.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
But the example you're bringing up is one of the great deal of upfront, pre-negotiations, and I think we want to establish a level of—I hate to use the term level of assurance, but in sort of the generic sense of the word the level of assurance that the holder of a certificate probably is legitimate organizationally that doesn't involve our having agreed that I like their HIPAA policies for what they're going to do with an employee who spills the beans.

Paul Egerman – Software Entrepreneur
How do we do that, Wes? How do you develop that sort of like without a contract? What are the components to do that?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
The questions we are answering right now establish a level of assurance. We're trying to find the questions to … level of assurance that this is at least a doctor or another healthcare entity, even if we don't know what the doctor—so we believe—it's an entity that has legal requirements imposed on it for the care and handling of personal health information. I would suggest that we substitute that for a common set of detailed agreements of exactly what the policies are for dealing with violations, which is the level of the DURSA. I would suggest that we would want to say that there may be individual cases where we want assurance to exceed that. But if we can establish this base level, we can at least move forward.

Paul Egerman – Software Entrepreneur
You have to establish the valid group practice or valid hospital or ….

Deven McGraw – Center for Democracy & Technology – Director
A valid DME supplier, a valid ….

Paul Egerman – Software Entrepreneur
A valid entity.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
By the way, be very careful about valid DME supplier because, with all the Medicare fraud stuff that's going on right now, some people would argue that we have no confidence in some of these DME suppliers.

Deven McGraw – Center for Democracy & Technology – Director
Yes. I don't know that we can fix all the problems with this.

Paul Egerman – Software Entrepreneur
Who said that? Was that Micky?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
It was John Houston. My editorial insight, sorry.

Paul Egerman – Software Entrepreneur
It's a great comment, John. Should we take them off the list?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
No.

Deven McGraw – Center for Democracy & Technology – Director
No.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
No, you can't take them off the list. It's very important. I think it just puts the burden of knowing that the person is appropriate to receive the information is not established by their possession of a credential.

Deven McGraw – Center for Democracy & Technology – Director
Right.

Paul Egerman – Software Entrepreneur
Either that or it has to be established in order to issue the credential.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Actually, we could figure out ….

David McCallie – Cerner Corporation – Vice President of Medical Informatics
But that's too hard. I think that's just too hard to do.

Deven McGraw – Center for Democracy & Technology – Director
I think we have to be very careful about relying on the credentialing process to enforce all of our laws.

Paul Egerman – Software Entrepreneur
Right. The credential just tells you that they are who their name says they are, that you weren't spoofed.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
However, I think it's interesting because this is a huge issue just based upon the fraud that we're hearing about.

Deven McGraw – Center for Democracy & Technology – Director
Undoubtedly, and certainly if somebody was in violation of a law or was committing fraud, there ought to be some process by which their credentials can be revoked.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Absolutely.

Deven McGraw – Center for Democracy & Technology – Director
Some connection between the two, in my view, but to establish the credential and require this sort of proof, not just of valid, physical existence, but also that you have a valid license to practice in the case of a doctor, or you have a hospital license that's in effect and has been appropriately renewed, or that you are not a DME supplier who in fact is defrauding the federal government. That's a pretty deep level of authentication.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes, I think we know that if in fact it was all that routine for the volumes of DME suppliers that are in the country to do it that at least the private payers would have done it and probably Medicare would have too. But the question I have is do we want to take the loop beyond this is a valid business entity because you can get a business license by being a person who is operating a DBA, and that's perfectly legitimate. Is this a valid business entity? That, I think, we sort of assume we're going to do that much. Is it a business entity that is engaged in a healthcare enterprise that would make it … we certainly know it's going to

claim to be one. Do we want to attempt to verify in any way that this is a business entity that's associated that's operating a healthcare business? That's the second question.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Then the third question is do we care to prove that they're competent and not defrauding operating as a healthcare entity? I don't think we can go that far.

Paul Egerman – Software Entrepreneur
Yes, but let's at least look at the second question that Wes is saying. Besides business entity, do they have to prove that they're a valid healthcare business entity? Is that what you're saying, Wes?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I'm trying to come up with a series of levels we can look at to answer those questions. I think we all agreed that we want to know it's a business entity ….

Deven McGraw – Center for Democracy & Technology – Director
Wes, I'm having trouble hearing you.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Fundamentally, I don't know exactly how to determine that it's business entity engaged in healthcare … personal visit. At that point, at least we know if it's something … claim as participating in healthcare, we don't really know even with a visit. But it definitely increases some level of assurance ….

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Wes, a minute ago you used a formulation that I thought made a lot of sense. You said an entity that was qualified to manage individually identifiable health information. Is that a better rubric than healthcare entity, because there could be entities out there that aren't traditional providers, but who are in fact authorized to handle and properly do handle individual health information?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I guess the question that that formulation raises is how you define qualified. If in fact you're saying an entity that is operating that has a goal or mission that would qualify it to maintain personal health information, then I would say that's more reachable. But even then, the process of going through and defining what that means would be difficult. Qualified has a current HIPAA security inspection or so forth. That's more than we want for this level.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
But I agree that that's a good constraint or that's a good issue, a real issue. But I think that there may be entities in the future that do not fit the current definitions of provider groups or any of the other things that we listed there like DME vendors that are in fact, on behalf of a consumer or provider, processing health information for some particular purpose, maybe making recommendations about treatment optimization like says the Keys Web site or a variety of other drug optimization Web sites where one electively chooses to directly message them with IHII and receive a service in return. It may not be anything like a traditional provider entity.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I agree. I think PHRs are just the leading edge of that.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Anything that receives its fundamental authority to have the data from the patient rather than from a provider is going to be in this new category.

Deven McGraw – Center for Democracy & Technology – Director
I have been noodling around with a couple of thoughts. One being that we sort of have set up some ideals about who we want to be suitable to get a credential here that we don't necessarily have good, strong definitions for. One is that they're a legitimate business. That one might actually not be that hard, but the second is that they are engaging in transactions that advance healthcare goals in the healthcare system, that they're not performing false transactions. That they're actually sort of a part of the healthcare system, and we're reluctant to sort of create, to use necessarily existing measures of validity like a provider number for Medicare, for example, because it feels confining because those are the entities that exist today, but it might not be the future.

We sort of have this high level agreement about what types of entities we want to make sure get credentialed. I wonder if rather than trying to grapple with the issue of what should they prove and what should they present, and what might we rely on that already exists in the marketplace to prove this? I hate skipping questions, but I wonder if instead we put the liability for getting that right on the entities that issue the credentials versus trying to dive down deep at this level and say, well, you have to prove X or Y or Z.

Paul Egerman – Software Entrepreneur
Yes. What you're suggesting is correct. Whatever we put down for requirements, the obligation of making sure that the requirements are met will be met by the certificate ….

Deven McGraw – Center for Democracy & Technology – Director
Well, that's right, and I guess ….

Paul Egerman – Software Entrepreneur
… organization.

Deven McGraw – Center for Democracy & Technology – Director
… but rather than going down the rabbit hole of figuring out the requirements, we ….

Paul Egerman – Software Entrepreneur
Well, that's right. You can just ….

Deven McGraw – Center for Democracy & Technology – Director
… the liability to those entities and worry less about being precise of what they have to get.

Paul Egerman – Software Entrepreneur
Well, maybe what you do though is you could put it at a high level, so those two high level comments I just heard you say. One is you have to have evidence you're a valid business entity. The second one is you have to have evidence that you already are processing healthcare transactions. All we have to do is say something like that. Evidence you're processing healthcare transactions, and maybe that's not exactly the right wording, but we don't have to say what that evidence is.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I'm curious. When the NHIN workgroup was in place, we got pretty far down the road of using the national provider identifier as a first step in the credentialing process or at least thinking about it that way. Given the track of questions now and the way the conversation has gone, I guess I'm wondering why that isn't part of the discussion.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

In the Direct conversations, we came up with a long list of people who don't actually get those identifiers issued to them. I don't know, for example, that nursing homes get them or DME vendors.

Paul Egerman – Software Entrepreneur
Let me respond to your comment, Carol. Suppose we define the requirement at a high level as evidence that you process healthcare transactions, or evidence that you're a healthcare entity, and suggest that an NPI might be one vehicle for accomplishing that.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
The reason I raise it is not because maybe it fits. It's more because government has to make that system work in order to pay bills. It seems to me that in order to pay someone, there is a level of credentialing or verification that has to go on. I guess I'm suggesting it because the more we can bootstrap on an existing mechanism, the more it is realistic. The more there are new or different mechanisms for administrative processes that need to be put in place, the more unlikely it is.

Paul Egerman – Software Entrepreneur
Let me sort of look at this one step at a time. The first step I like to say is do we agree that there has to be some evidence that this is a healthcare entity, that it is processing healthcare transactions? That that's got to be one of the requirements?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Yes.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Paul Egerman – Software Entrepreneur
Then the question is what Carol is saying. Can we be more specific and say it has to have an NPI, or is it just adequate to say it has to provide evidence that it's a valid healthcare entity?

Deven McGraw – Center for Democracy & Technology – Director
I think it's actually a little more than that. I think maybe there's another recommendations, which is to suggest that we do bootstrap onto existing processes where it's appropriate. So an NPI is not going to work for the universe of exchangers, but it's going to work for a bunch of them.

Paul Egerman – Software Entrepreneur
So maybe it's a third thing. Well, does the existence of an NPI, if an entity says I have an NPI, is that a valid response to proof that you're a valid healthcare organization?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Yes.

Paul Egerman – Software Entrepreneur
Okay. So the second criteria is you have to prove that you're a valid healthcare organization using NPI or using NPI plus or using NPI if applicable?

Deven McGraw – Center for Democracy & Technology – Director
Yes, that's one mechanism for proof is that you have to prove you're a healthcare organization or enterprise or transacting healthcare business, and the issuers of digital credentials should bootstrap on existing processes as much as possible, and the NPI would be one of them.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
But we don't want to exclude things like DME and personal health records, right?

Deven McGraw – Center for Democracy & Technology – Director

That’s right. That’s right, so I tried to word it in a way to suggest that we’re not requiring everyone to have an NPI to get a credential, but saying that you have to prove you’re a healthcare, an entity who is transacting, who is exchanging PHI as part of being for healthcare purposes, and we want to bootstrap onto existing processes to prove that point where possible, which includes the NPI in places where the entity would have to have one.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I want to be clear though that the NPI is something that people can look up, and it’s available. That is not the token for authentication. I guess I want to make sure we’re not going down that.

Deven McGraw – Center for Democracy & Technology – Director
Right.

Paul Egerman – Software Entrepreneur
Yes. No, that’s ….

Deven McGraw – Center for Democracy & Technology – Director
I think we’re talking about proving that the entity is a healthcare entity.

Paul Egerman – Software Entrepreneur
Before you issue the credentials.

Leslie Francis, NCVHS – Co-Chair
If you’re going to pick up on Paul’s point though about PHR providers, there are some of them that I don’t think are required to have business associate agreements or that might be if the July NPRM becomes final, but that have not been traditionally, in the healthcare system anyway, processing healthcare information.

Deven McGraw – Center for Democracy & Technology – Director
Leslie, that’s right, which is why we don’t want to require an NPI of everybody, right? But we do want ….

Leslie Francis, NCVHS – Co-Chair
… processing healthcare information might sound similarly limiting. That’s all.

Deven McGraw – Center for Democracy & Technology – Director
Okay. Do you have another suggested way to word it? We can work on it offline too.

Leslie Francis, NCVHS – Co-Chair
But it’s people who have legitimate reasons to be participating in meaningful use is what you’re looking for.

Paul Egerman – Software Entrepreneur
Interesting.

Deven McGraw – Center for Democracy & Technology – Director
I mean, if we did focus on the universe of entities that are going to be participating in meaningful use, we certainly would be directing our recommendations toward the policy tools that ONC has at its disposal.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Which is a nice thing to keep in mind.

Paul Egerman – Software Entrepreneur
Where are we?

Deven McGraw – Center for Democracy & Technology – Director

I think we are at the point of saying that we want, I mean, maybe we didn't hear enough back from folks on meaningful use. It seemed like a good suggestion that we didn't hear folks push back on, so if in fact that was amenable, in terms of the requirements at a high level, being a valid business entity and be exchanging health information in furtherance of the meaningful use criteria.

Paul Egerman – Software Entrepreneur
And that's ….

Deven McGraw – Center for Democracy & Technology – Director
And … to existing mechanisms to help prove that they are in fact entities that are officially doing this, and the NPI would be one, but that's not an exclusive list.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Maybe this is a technicality, but it's really the activities covered by meaningful use as opposed to specifically seeking stimulus rewards under meaningful use.

Deven McGraw – Center for Democracy & Technology – Director
Yes. That's right.

Paul Egerman – Software Entrepreneur
Is there anything else that we want to put as requirements?

Deven McGraw – Center for Democracy & Technology – Director
It's a good set for now.

Paul Egerman – Software Entrepreneur
There was one other comment that's written on this screen, which is, let's go back to 2B if we can ….

Deven McGraw – Center for Democracy & Technology – Director
Sorry. I'm so excited, Paul, and I moved us ahead.

Paul Egerman – Software Entrepreneur
I know. There was a second bullet here. I just want to make sure we hit the second bullet. It mentions that the credentials are electronic. Do we want to put forward any registration requirements for receiving the credentials that might be considered? For example, do you want to say there needs to be an in-person visit by a business representative, or do we just not want to touch that issue?

Deven McGraw – Center for Democracy & Technology – Director
It feels a little in the weeds. I think I'd rather look to what entities are going to be performing this and give them the liability for getting it right, but some flexibility about how they do it.

Paul Egerman – Software Entrepreneur
Any other comments?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Don't the NIST levels of assurance segregate some of these details? Do we end up eventually picking a NIST level?

Paul Egerman – Software Entrepreneur
We sort of already went through that because we're not going to actually pick a NIST level from the organizational credentials.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I like what Deven just said. We hold the credentialing organizations liable. But is there law in place that would hold them liable?

Deven McGraw – Center for Democracy & Technology – Director
Yes, that's a good question, Dixie. We may need to create that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
… right approach, but ….

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I think this is the key to this whole issue, which is, if there isn't an oversight mechanism that is transparent and where gaps in the way the system is working or breaches or what have you or fraud not visible to participants, the whole system kind of quickly degrades, right, because you start to not trust the credential. I think that's a critical element of this.

Deven McGraw – Center for Democracy & Technology – Director
Agree.

Paul Egerman – Software Entrepreneur
But on this issue, I don't hear anybody saying yes, we want to put forward this kind of requirement.

Deven McGraw – Center for Democracy & Technology – Director
Yes, I don't think so.

Paul Egerman – Software Entrepreneur
Let 's move on to the next slide. I think you're going to do the next one, Deven.

Deven McGraw – Center for Democracy & Technology – Director
This next question, this is another question in two parts. Three A is what is the process for issuing digital credentials. As you'll see, some of the suggested responses here engage at whether this is sort of a federated or distributed model or whether there ought to be a sort of straw role for the federal government in this space. And just to look ahead to see what 3B is, that's process for reevaluation, not that that's not important, but 3A, this is a pretty tough question, I think.

We already said, keep in mind that in our tiger team recommendations that were accepted over the summer, we had said that providers are always ultimately responsible for the security of the health information they exchange, but they can certainly delegate to other parties the responsibility for issuing digital credentials, for example, as long as they do so in a trustworthy manner. Are we looking at an environment? I think there's a threshold question to be answered here. Are we looking at an environment where there would be multiple parties issuing digital credentials?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
You would hope if there were that it would follow this sort of e-gov model, which is to certify the certifier approach.

Deven McGraw – Center for Democracy & Technology – Director
Yes. Well, I think that would be an important statement to make that while maybe we do need to have the ability for multiple entities to be able to credential, which is the case today, but there ought to be some mechanism, whether it's through certification or some other form of governance, for assuring that these entities that issue these credentials are doing so appropriately, securely, etc. Is that the answer?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'm not sure what you're addressing in this first bullet. I don't think the act of proving that you're a health organization should be something you can delegate. However, once you get that credential, then I think you certainly can delegate to a business associate to take actions on your behalf and under that credential.

Deven McGraw – Center for Democracy & Technology – Director

I think it's more of the question, Dixie, of you as a provider have to prove you are transacting healthcare information in furtherance of the goals of meaningful use. Somebody has to judge that you've done that, that you qualify. And so the question is about who those entities are.

Paul Egerman – Software Entrepreneur
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I don't think ….

Deven McGraw – Center for Democracy & Technology – Director
Yes, I'm sorry if it's not clear from the statements.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
There is a lot of precedence, existing protocols you refer there, the federal bridge and ICANN.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Are those deemed inadequate in some way? Are they too top heavy, or do we have feedback maybe on the blog suggesting that those are not working?

Deven McGraw – Center for Democracy & Technology – Director
I think a lot of the comments that we got on the blog were to a number of commenters, certainly not all, suggested that credentials could be issued through multiple entities, including vendors that ICANN and the federal bridge would not be the sole spots of reliance on credentials issuing. We did get comments that it's too top heavy. Of course, we also got comments of people recommending that we require more of a centralized process.

Paul Egerman – Software Entrepreneur
I'd respond a little differently, David, because I think basically we can sort of set up a structure where we can define exactly who is authorized to issue certificates, but it doesn't have to be the usual players. If we wanted to, we could define it in such a way, for example, that the HIOs would be the ones who issued the certificates maybe perhaps using the argument, well, they're the ones who are most likely to know who are the healthcare entities in their region. That would be a good way to avoid fraud. I use that as an example. Another example is that you could define that large organizations like UPMC or Kaiser could issue certificates if they met certain criteria because also they know who are the healthcare entities in their region. So we could define it however we want to, but ….

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Without getting into a lot of detail, I think that that's a model that's going to become most workable, especially when dealing with things like business associates because we may say that we can issue a credential, and it's going to be what I would deem as a sub-credential underneath me. So I've got to vouch for that organization, and that organization is really, its purpose would be to conduct business maybe on behalf of me or for me, but it would be clear that my credentials are part of that. UPMC's credentials are part of the larger credential that's being sent around, I guess, if that makes sense.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. I think my question was answered, which is that we are leaning strongly, it sounds like, towards a federated model, but perhaps one that is broader than the existing federal bridge entities.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
ICANN doesn't do credentials. It does IP addresses. Most credentials today, like machine certificates, are done by like VeriSign companies.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. Correct, and what I'm suggesting, Dixie, is we can go with that as a concept, or we could go with something that I would describe as more restrictive. We'd say instead of just a security company, we can define rules in such a way that the security company could do it, but you would define rules in such a way that not everybody can necessarily issue the certificates.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Maybe we put them under the certification mechanism that's already being created for EHRs.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Well, you can't. The certification mechanism for EHRs only works for EHRs. We can't certify whatever we want to certify.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
You can't build on that? I know it's not an EHR.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
No, you can't. But what you can do is you can define. We can define our own. We can define the rules by which somebody receives a certificate, and we can actually define some information about the process. One suggested response to this question could be to say we want multiple issuers of certificates, and we would like the certificates to be regionally based and have to be organizations that have knowledge of the existence of healthcare organizations.

Deven McGraw – Center for Democracy & Technology – Director
It still feels to me … it feels a little cramped to me. I guess I keep gravitating to a solution that allows a number of entities to issue digital credentials as long as they can either submit themselves to a certification process so we can be sure that we trust them and have some sort of governance over their assumption of the liability of getting it right rather than narrowing it at that end. But I don't ….

David McCallie – Cerner Corporation – Vice President of Medical Informatics
One minor thing, Deven, let me suggest we use the word accreditation instead of certification. We want to separate it from the certification process.

Deven McGraw – Center for Democracy & Technology – Director
Yes. We have a governance/accreditation process for assuring that these digital credential issuers are being diligent in how they operate, but that we not necessarily try to confine who they could be.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
It would be multiple issuers and an accreditation process.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Can I also suggest that we speak to the fact that there are different classifications of certifiers or credentialers that again some might be for UPMC being able to certify a business associate for my purposes versus an HIE that might certify somebody for regional access.

Deven McGraw – Center for Democracy & Technology – Director
I don't understand what you mean though, John. How would that look like? What would that look like from a policy standpoint because that looks different to me than the suggestion that I had, which is to create the governance. To sort of create the accountability at the higher level, but allow entities to create their, to allow multiple entities to digitally certify, which would mean you could digitally certify your own business associates.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Yes, but I guess it's a question of scope then. I think that I can digitally certify my business associate, but the scope of that business associate's right would be when it's conducting business on my behalf. I don't

want to necessarily digitally certify a business associate for its entire business operation independent of which covered entity it's providing services to.

Paul Egerman – Software Entrepreneur
Not to interrupt, but when you said digitally certify, you mean digitally credential?

Deven McGraw – Center for Democracy & Technology – Director
Yes, I'm sorry. That's what I meant.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
But, John, are you talking about different sort of levels of trust being implied by what kind of an entity issues a credential?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I'm not sure whether trust is the right concept as it's scope of use. Yes. I guess you could say, again, if it's a business associate, and UPMC is vouching for that business associate, it's for the scope of UPMC's business purpose.

Paul Egerman – Software Entrepreneur
Yes. My response to that, John, would be if you want to do that, that's fine. But that's a different kind of credential. We're talking about a digital credential that in effect says this entity is valid on the NHIN or NW-HIN, whatever the correct initials are, and people should feel some level of minimal assurance in communicating with it.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I understand that; believe me.

Paul Egerman – Software Entrepreneur
So that's what it is. It's not just for UPMC's use. It's for other people's use also.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
The but to that though is that if I've got a business associate acting on my behalf, the extent to which I should be able to credential that business associate, and the degree that others should trust them, is within the scope of UPMC's relationship with that business associate. Once it extends beyond that, that business associate needs to have—potentially has multiple credentials based upon the services that are provided to different covered entities. Again ….

Deven McGraw – Center for Democracy & Technology – Director
Yes, but that sort of sounds to me like, John, it's more than about a digital credential and about sort of a set of permissions, maybe access controls with respect to what type of business they're able to transact on your behalf that's going to be different for you than it might be for other covered entities that they serve.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Absolutely. Maybe I'm engineering a solution, but I just think about this, and I think if that business associate is participating through their association with me, that should be the only context in which they should be transacting business.

Deven McGraw – Center for Democracy & Technology – Director
Except what if that business associate is SureScripts?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Then SureScripts may, as a business associate, have to have credentials for every organization it participates with. Again, I think of it as sort of like sub-credentials.

Paul Egerman – Software Entrepreneur
… hard.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
… credentialing process at some regional level, but if I've got hundreds of business associates, and I'll vouch for them in the context of what they're doing for me, but I don't want to vouch for them generally as part of this large network.

Paul Egerman – Software Entrepreneur
I think what you're saying might be the case that UPMC doesn't want to vouch for them generally, and so that could be your decision. However, what we're trying to design here is a situation where you don't have to have individual credentials for each point-to-point of communication because otherwise we're going to have more credentials than we have healthcare organizations in the country by orders of magnitude. It's exponential in terms of all the possible connections.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Maybe, again, and during the technical design, but maybe business associate is one credential, but when it's transacting, it has to also supply the credential of the organization it's ….

Paul Egerman – Software Entrepreneur
Well, you're starting to get into some of the details of what the content of the message is. But right now we're just trying to make sure that the digital credential accurately identifies who you are.

Deven McGraw – Center for Democracy & Technology – Director
You are. Right.

Paul Egerman – Software Entrepreneur
So we've got to keep that in mind. That's our focus.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
It's really that we're sort of saying who you are, that you are who you say you are, and some minimum level of appropriateness. What we're struggling with is what's the minimum level of appropriateness, such as ability to handle patient health information in an appropriate way. That's the language we've been wrestling with.

Paul Egerman – Software Entrepreneur
That's right. Thank you for reminding us of that, David, and those are very appropriate comments. I appreciate that, David. Getting back to the question, the question is this concept of process. It's an interesting question. What Deven has put on the table is to say, well, there could be multiple authorities that can issue these certificates. There needs to be some accreditation process or organization to make sure that they do their job right. That's what you're saying.

Deven McGraw – Center for Democracy & Technology – Director
Yes, that they're accountable for doing it right, that they're taking on some liability for issuing credentials to the right entities.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think that's absolutely right. I would also add that the credentials need to be – there has to be some cross-certification in there as well so that if I go to VeriSign to get my credential, I'm not limited to exchanging health information only with others with VeriSign credentials.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Leslie Francis, NCVHS – Co-Chair
Accountability and liability are different too, and I want to make sure you know which one you mean or both.

Deven McGraw – Center for Democracy & Technology – Director
Tell me what you think the distinction is, Leslie, because I might mean both.

Leslie Francis, NCVHS – Co-Chair
Accountability would mean that someone checks up on you. You report to them that you're doing it appropriately, that you're meeting standards.

Deven McGraw – Center for Democracy & Technology – Director
I mean both.

Leslie Francis, NCVHS – Co-Chair
But it can take away your power. Liability, I was thinking in terms of the possibility to sue for damages if you erroneously credential or negligently credential, don't check up on, and then they're harmed.

Deven McGraw – Center for Democracy & Technology – Director
I definitely meant accountability. I certainly think that in order to be validly issuing someone digital credentials that whether it's through a registration process or some sort of way that we know we can hold you accountable, and we can revoke your accreditation, for example, to issue digital credentials as part of the NW-HIN, NHIN. I don't know that we have any authorities to be able to impose the kind of liability that you've suggested, absent that it might exist to some extent already.

Leslie Francis, NCVHS – Co-Chair
I wasn't suggesting that we needed to do that, but use accountability then not liability as ….

Deven McGraw – Center for Democracy & Technology – Director
Yes. Okay. Thank you, Leslie.

Paul Egerman – Software Entrepreneur
Do you want to say it one more time to make sure we're all in agreement, Deven?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Yes, Deven. Say it one more time.

Deven McGraw – Center for Democracy & Technology – Director
I'll try. I have some notes here. They're not perfect. I think we're talking about multiple entities being able to issue digital credentials, but we want there to be some accountability, such as through an accreditation or some other form of governance for those entities who issue digital credentials so that there's some level of assurance that they are performing authentication appropriately.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
It's actually performing credentialing appropriately.

Deven McGraw – Center for Democracy & Technology – Director
Yes. Thank you.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I would just say that the annual sort of accreditation or validation that someone is performing it appropriately is probably inadequate for what we're after. I think we'll have to flush this out to include some level of observability and transparency so that any lapses or breaches are quickly seen and identified.

Deven McGraw – Center for Democracy & Technology – Director
Yes. Good points. We're making good progress.

Paul Egerman – Software Entrepreneur
We are. We're actually almost right exactly on schedule.

Deven McGraw – Center for Democracy & Technology – Director
Yes. It's interesting. Three B is a process for reevaluation, but I'm wondering and, Paul, you can feel free to push back, whether we've actually answered question four, which is, who can issue digital credentials.

Paul Egerman – Software Entrepreneur
Let's do 3B first.

Deven McGraw – Center for Democracy & Technology – Director
I'd be happy to, except ….

Paul Egerman – Software Entrepreneur
Do you want to do four?

Deven McGraw – Center for Democracy & Technology – Director
Yes, because I think we actually just answered it. We dealt arguably more with the question of who than the process for credentialing. I'm not sure what we wanted. If you look back at the precise wording of question 3A, it's a process for issuing digital credentials, and yet even some of the recommended answers that we have here led us into a discussion that looked more like—and I'm skipping ahead to number four—who can issue digital credentials where we've got any entity willing to assume the risk and then establishing an accreditation program for that. This is not to suggest that we don't take on 3B next, but I think we arguably answered number four. I'm not sure what else we would say about a process for issuing credentials beyond what we've already said. If I've thoroughly confused everyone, we can go back to 3B. But I think we actually got to number four.

Paul Egerman – Software Entrepreneur
I think so too.

Deven McGraw – Center for Democracy & Technology – Director
Which is nice. It's an interesting way to make progress is to skip questions and that it looks like you went farther. The question 3B is about sort of reevaluation, and I think at the heart of this question is how long do we think a digital credential ought to last before it has to be refreshed or reissued?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Did we think that there should be the same rules for all provider entities regardless of how large they are or how much data they exchange or any other factors we might consider?

Deven McGraw – Center for Democracy & Technology – Director
I don't know, Dixie. I think that's a good question.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. I just had an interesting experience the other day that got a phishing attack via e-mail to Bank of America, very cleverly disguised, and it would take off many, many people, including people that know what they're doing. It was, in a matter of about 45 minutes, that Web site was taken down by some authority somehow, somewhere. I wonder if we have to approach that kind of responsiveness in this, if there are people abusing the system.

Deven McGraw – Center for Democracy & Technology – Director
I would hope so, David, personally.

Paul Egerman – Software Entrepreneur
Yes, I would hope so too, although that's a different issue than this issue. This issue is, whatever the process is…. Dixie raises a good point. Does UPMC, once a year for example, have to prove that they exist?

Deven McGraw – Center for Democracy & Technology – Director
It was John.

Paul Egerman – Software Entrepreneur
Right?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Or maybe certain classes of organizations need to, like business associates because they're servicing some other entity.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That, John, has the same question to me as if you're a business associate of a two doc practice, are your requirements the same as a business associate of UPMC?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Yes, you're right.

Leslie Francis, NCVHS – Co-Chair
That's the same. I don't think you can have a lower standard just because you're smaller.

Paul Egerman – Software Entrepreneur
I agree.

Deven McGraw – Center for Democracy & Technology – Director
Yes. In fact, the smaller entities may come and go more frequently.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, but if I'm able to fake, to convince somebody that I'm Kaiser, I can do a heck of a lot more damage more quickly than if I convince them that I'm this dentist down here at the corner.

Deven McGraw – Center for Democracy & Technology – Director
Do the points you're making go to how often it should be reevaluated? If so, what would you suggest?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I just now thought of it, but I think it goes to both, the level of proof that you have to show, but certainly how often you have to. Yes, you may be right. It might just have to do with how often you have to. Maybe that's the difference. Does it just have to do with how often you have to be reevaluated?

Deven McGraw – Center for Democracy & Technology – Director
Right.

Paul Egerman – Software Entrepreneur
I'll just throw out one year. Everybody has to be evaluated one year … Leslie said. What do people think of that?

Deven McGraw – Center for Democracy & Technology – Director
Every year?

Paul Egerman – Software Entrepreneur
Every year.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I'm a little lost in this conversation. Who are we talking about being reevaluated, the credentialee or the credentialer?

Deven McGraw – Center for Democracy & Technology – Director
No.

Paul Egerman – Software Entrepreneur
The "we," the healthcare organization. The recipient of the credential. Sorry, the person who, the entity that was issued the credentials would have to prove that they're still a business entity and they're still a healthcare organization.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I would assume that would be the minimum, to go back to David's original point. There has to be a mechanism for ongoing identification of misuse or breach.

Deven McGraw – Center for Democracy & Technology – Director
Yes. That gets to your transparency point, Carol, in that we not just rely on refreshing or even accreditation on an annual or however many year basis is the sole mechanism of accountability here.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Right.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Just a question here. I'm thinking that we're talking about something on the order of a half a million entities. Are other people thinking the same scale?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
That's probably about right, maybe even bigger.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes, so a half a million annual revalidations that say it cost $50 is $5 million a year. I guess that's an acceptable cost.

Deven McGraw – Center for Democracy & Technology – Director
Yes, and especially when we're talking about multiple digital—that we're not trying to send everybody through a pretty narrow pipeline.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Maybe we put some wiggle room into this by saying unless the organization can be otherwise verified, we have to be recredentialed every year. The reason why I say that is let's just say you have a provider that bills Medicare, and you link their Medicare information up with their credential so that we know that they still exist because they're still doing Medicare billing.

Deven McGraw – Center for Democracy & Technology – Director
But it would be very easy to reissue that.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Right.

Deven McGraw – Center for Democracy & Technology – Director
But by saying annual, there's a process in place whereby that sort of check the box gets done.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Are there other thresholds like change of ownership, things like that?

Deven McGraw – Center for Democracy & Technology – Director
Good point.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I got a beep as he was talking. What did he say? Such as what?

Deven McGraw – Center for Democracy & Technology – Director
Change of ownership.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Good point.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Why would a change of ownership cause you to be reevaluated?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I guess only if it results in a different DEA number or something, or a different billing number or something.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
If you have a different – the name of the entity or the entity….

Deven McGraw – Center for Democracy & Technology – Director
Well, if the entity changes ownership, and they change functions.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Well ….

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Yes.

Deven McGraw – Center for Democracy & Technology – Director
It'd have to be a significant change of circumstances that put into question the two broad criteria that we set out at the beginning that you're a valid business and that you're involved, engaging in the exchange of health information for the activities that support meaningful use.

Paul Egerman – Software Entrepreneur
Or, to put it differently, if any of the information you provided to get the certificate, the credential changes, then that would be the reason for doing it.

Deven McGraw – Center for Democracy & Technology – Director
Right.

Paul Egerman – Software Entrepreneur
For recredentialing.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, that sounds good.

Paul Egerman – Software Entrepreneur
Have we got this one year, or if there's a change in your ….

Deven McGraw – Center for Democracy & Technology – Director
In the information.

Paul Egerman – Software Entrepreneur
In the evidence. In your information that ….

Deven McGraw – Center for Democracy & Technology – Director
Yes. Should we say material change, so if you just changed your doing business as address, you shouldn't necessarily have to trigger it, physical address?

Paul Egerman – Software Entrepreneur
I think that's the attorney ….

Deven McGraw – Center for Democracy & Technology – Director
All right. That's fair. I think we got through four, and we need to do some public comment, Paul.

Paul Egerman – Software Entrepreneur
I think this is great, and before we start the public comment, I'd just tell you that ….

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Can I just say one thing before we break? I feel like this last set of requirements is delving into areas that we're probably not the best group to figure out, and I wonder if we could think about reshaping them in terms of bars that have to be hit or criteria as opposed to the actual requirement.

Paul Egerman – Software Entrepreneur
Those are good comments because we do have another meeting on this Friday, the 15th. Is that right? Is that the right date?

Deven McGraw – Center for Democracy & Technology – Director
No. It's the 12th.

Paul Egerman – Software Entrepreneur
Sorry, Friday, the 12th. What we're going to be doing is we'll do what you just suggested, Carol. We'll also review where our recommendations are, and then we'd be looking at questions five and six, which deal with some interesting issues about certification and meaningful use and what transactions, but we've made great progress this morning, so I appreciate everybody's participation.

Does anybody else have anything else to say before we open it up to public comment? Judy, if we could do the public comment, and then Deven will do the close.

Judy Sparrow – Office of the National Coordinator – Executive Director
Operator, if you could see if anybody would like to make a comment from the public. The lines can be opened.

Coordinator
We don't have any comments at this time.

Deven McGraw – Center for Democracy & Technology – Director
We must have exhausted everybody in the FACA blog. We will get out some language that is our attempt to synthesize where we think we were on the previous questions and endeavor to make more progress on what remains on our next call on Friday. Thanks to everyone for your participation today. As usual, a great call, and see you later in the week.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Great. Thanks a lot, Deven and Paul.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you.

Public Comment Received During the Meeting

1. NPI works well for HEALTH PROVIDERS... but they are talking to OTHERS that are NOT providers. And NPI is POORLY credentialed, and has no expiration or revocation.... and is NOT a digital certificate. The RECOMMENDATION could be that the NPI process MUST add good provisioning/credentialing mechanisms, issues digital certificates, and has a revocation mechanism.... This would be great recommendation to HHS/ONC. Your POLICY should not lock in ONE or a FEW certificate authorities... Write Policy that others use to make decisions. Manual (self-signed certs) are legitimate technology when used properly. Don't act like you know better than everyone else.

2. The main problem the group is struggling with is the lack of any existing central authority. There will not be a central authority in technology if there is none in non-technology.

3. Need to separate the concept of Identity from Authentication from Authorization... These ARE three different but related things.

4. All communications of PHI must be mutually-authenticated to XYZ Policy on identity assurance.

5. When Organizational or System level authentication is used   XYZ Policy defines the identity assurance necessary.

6. Digital credentials for a machine DO NEED a level of assurance policy! We can't have systems claiming they are authenticating because they are using an IP address.

7. Please keep this RISK based... the question is 'what is the risk' being addressed by some technology/policy.

8. Use-case: Directed exchange (the Direct Project) uses user-level certificates to provide end-to-end authenticity/confidentiality/integrity... is there really MORE needed? Meaning is there really a need for also machine-to-machine authentication? I don’t think so.

9. Please don't forget about setting policy for BOTH ends of a communications. It is just as important to authenticate the sender as it is to authenticate the receiver.